DOCKET NO. FIN0004-CIP3 -PAT **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Moshe RUBIN, et al. Group Art Unit: 2165

App. Serial No.: 09/459,493 Examiner: Hassan Mahmoudi
Patent No.: 7,281,272

Filing date: December 13, 1999
Issue date: October 9, 2007

For: METHOD AND SYSTEM FOR COPYRIGHT PROTECTION OF DIGITAL IMAGES

REQUEST FOR CERTIFICATE OF CORRECTION

U.S. Patent and Trademark Office
Customer Service Window
Attn: Certificate of Correction Branch
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

The undersigned requests that a Certificate of Correction be issued for the above-identified patent as indicated on the attached Form PTO/SB/44 (04-05).

This request is being made in order to correct the foreign priority information for this patent. Three (3) foreign applications/patents (IL 124895, IL 127093, and IL 127869) need to be added to the Foreign Application Priority Data (30) section of the patent.

The present application claims priority to and is a continuation-in-part of U.S. Application No. 09/397,331 (now U.S. Patent No. 6,298,446), which claims priority to foreign application/patent Nos. IL 127093 and IL 127869, and which is a continuation-in-part of U.S. Application No. 09/313,067 (now U.S. Patent No. 6,209,103), which claims priority to foreign application/patent No. IL 124895.

Pursuant to MPEP 201.16, a Certificate of Correction can be filed to perfect a claim of foreign priority benefits based on the satisfaction of the requirements of 35 U.S.C. 119(a)-(d) or (f) in the parent application. These requirements were met in parent application Nos. 09/397,331 and 09/313,067, and we request that foreign application/patent Nos. IL 124895, IL 127093, and IL 127869 be added to the present patent. The entire delay between the date the priority claim was due and the date of the claim filed (herewith) was unintentional as to the present patent.

With regard to foreign applications/patents Nos. IL 127093 and 127869, these applications/patents were cited in the executed Declaration filed in the parent application, and the claim was perfected on September 18, 2000 with the filing of the certified priority document for each of the foreign applications/patents. A copy of the executed Declaration is attached as Exhibit A. A copy of the foreign certified priority documents filed in the parent application are attached as Exhibit B. On May 2, 2001, a Notice of Allowance was mailed by the U.S. Patent and Trademark Office in which the Examiner acknowledges the claim for foreign priority and acknowledges receipt of the certified priority documents. A copy of the Notice of Allowance is attached as Exhibit C.

With regard to foreign application/patent No. IL 124895, a copy of the certified priority document is attached as Exhibit D.

Pursuant to MPEP 201.16 a Petition for Unintentional Delay of Priority Claim is not necessary as the present application was filed prior to November 29, 2000.

This Request for Certificate of Correction is being filed due to an error by the applicant. A fee of $100.00, pursuant to 37 C.F.R. §1.20(a), and a fee of $130.00, pursuant to 37 C.F.R. 1.55(a), is included herewith. However, the Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment, to Deposit Account No. 50-4402.

Respectfully submitted,

Date: August 25, 2011

By: */Dawn-Marie Bey - 44,442/*
Dawn-Marie Bey
Registration No. 44,442

KING & SPALDING LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006
(202) 737-0500

15157/105001
Doc. No. 17142397

Docket No.
6866-101C1

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND SYSTEM FOR COPYRIGHT PROTECTION OF DIGITAL IMAGES TRANSMITTED OVER NETWORKS

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on **September 14, 1999** as United States Application No. or PCT International Application Number 09/397,331

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
127093	Israel	November 16, 1998	☐
(Number)	(Country)	(Day/Month/Year Filed)	
127869	Israel	December 30, 1998	☐
(Number)	(Country)	(Day/Month/Year Filed)	
(Number)	(Country)	(Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

09/313,067	May 17, 1999	Pending
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Robert Berliner, Registration No. 20,121
Billy A. Robbins, Registration No. 18,313
M. John Carson, Registration No. 25,090
John M. May, Registration No. 26,200
Margaret A. Churchill, Registration No. 39,944
Terri A. Sale, Registration No. P45,066

Send Correspondence to:

Robert Berliner, Esq. - FULBRIGHT & JAWORSKI L.L.P.
865 South Figueroa Street -29th Floor
Los Angeles, CA 90017-2576

Direct Telephone Calls to: *(name and telephone number)*
Robert Berliner, Esq. - 213-892-9200

Full name of sole or first inventor **Daniel SCHREIBER**
Sole or first inventor's signature Daniel Schreiber Date 30/11/94
Residence **Beit Shemesh, ISRAEL**
Citizenship **ISRAEL**
Post Office Address **71 Shimon Street, Beit Shemesh 99543, ISRAEL**

Full name of second inventor, if any **Andrew GOLDMAN**
Second inventor's signature A. Goldman Date 30/11/94
Residence **Beit Shemesh, ISRAEL**
Citizenship **ISRAEL**
Post Office Address **73 Shimon Street, Beit Shemesh 99543, ISRAEL**

EXHIBIT B

SF

Date Mailed: 09/13/00 | Atty/Sec: DRB/ma | Filing Date: 09/14/99

Serial No.: 09/397,331 | Docket No.: 4692

Applicant(s): Daniel Schreiber and Andrew Goldman

Title: METHOD AND SYSTEM FOR COPYRIGHT PROTECTION OF DIGITAL IMAGES TRANSMITTED OVER NETWORKS

Please imprint Patent Office "date stamp" hereon to indicate receipt and then return card to addressee

- ☐ __ pages of Specification, Claims, & Abstract
- ☐ __ sheets of formal drawings
- ☐ Provisional Application Cover Sheet
- ☐ New Utility Application Transmittal
- ☒ Transmittal
- ☐ Fee Transmittal (in duplicate)
- ☐ Power of Attorney by Assignee
- ☐ Copy of Assignment & Recordation Cover Sheet
- ☐ Small Entity Statement
- ☐ New Design Application Transmittal
- ☐ CPA Request Transmittal
- ☐ Check in the amount of $ ___
- ☒ Other: Israeli application nos. 127093 and 127869
- ☐ Amendment/Response
- ☐ PTO-1533 & Resp. to Notice Of Missing Parts
- ☒ Certified Copy of Priority Document(s)
- ☐ Certificate Under 37 CFR § 3.73(b)
- ☐ IDS, PTO-1449, and cited references
- ☒ Return receipt postcard
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawings: __ sheets
- ☐ Maintenance Fee Payment
- ☐ Request for Certificate of Correction
- ☐ Notice of Appeal
- ☐ Express Mail No. ___

EXHIBIT B

PTO/SB/21 (modified)
Approved for use through xx/xx/xx, OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

0001/PTO
Rev. 10/95

U.S. Department of Commerce
Patent and Trademark Office

TRANSMITTAL FORM

(to be used for all correspondence during pendency of filed application)

Application Number	09/397,331
Filing Date	September 14, 1999
First Named Inventor	Daniel Schreiber
Group Art Unit Number	2785
Examiner Name	Bryce P. Bonzo
Total Number of Pages in This Submission: 48	Attorney Docket Number: 4692

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form (in duplicate)
  - ☐ Check Enclosed
- ☒ Return Receipt Postcard
- ☐ Response to Notice to File Missing Parts
- ☐ Assignment & Recordation Cover Sheet
- ☐ Declaration
- ☐ Small Entity Statement
- ☐ Information Disclosure Statement & PTO-1449
  - ☐ Copies of IDS Cited References
- ☐ Request for Corrected Filing Receipt
- ☐ Request for Correction of Recorded Assignment
- ☐ Amendment/Response: [ ] Page(s)
  - ☐ After Final
- ☐ Status Request
- ☐ Revocation and Power of Attorney
- ☐ Issue Fee Transmittal
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawing(s):
  - [ ] Sheet(s) of Figure(s) [ ]
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☒ Certified Copy of Priority Document(s)
- ☐ After Allowance Communication to Group
- ☒ Israeli application nos. 127093 and 127869
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

REMARKS:

SIGNATURE OF ATTORNEY OR AGENT

Signature:		
Attorney/Reg. No.:	Daniel R. Brownstone, Reg. No. P-46,581	Dated: Sept 13, 2000

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to the attention of Examiner Bryce P. Bonzo, Group Art Unit 2785, Commissioner for Patents, Washington, D.C. 20231 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.

Signature:		
Typed or Printed Name:	Daniel R. Brownstone	Dated: Sept 13, 2000
Express Mail Mailing Number *(optional)*:		

EXHIBIT B

Date Mailed: 09/13/00 | Atty/Sec: DRB/ma | Filing Date: 09/14/99

Serial No.: 09/397,331 | Docket No.: 4692

Applicant(s): Daniel Schreiber and Andrew Goldman

Title: METHOD AND SYSTEM FOR COPYRIGHT PROTECTION OF DIGITAL IMAGES TRANSMITTED OVER NETWORKS

Please Imprint Patent Office "date stamp" hereon to indicate receipt and then return card to addressee

- ☐ __ pages of Specification, Claims, & Abstract
- ☐ __ sheets of formal drawings
- ☐ Provisional Application Cover Sheet
- ☐ New Utility Application Transmittal
- ☒ Transmittal
- ☐ Fee Transmittal (in duplicate)
- ☐ Power of Attorney by Assignee
- ☐ Copy of Assignment & Recordation Cover Sheet
- ☐ Small Entity Statement
- ☐ New Design Application Transmittal
- ☐ CPA Request Transmittal
- ☐ Check in the amount of $ ___
- ☒ Other: Israeli application nos. 127093 and 127869
- ☐ Amendment/Response
- ☐ PTO-1533 & Resp. to Notice Of Missing Parts
- ☒ Certified Copy of Priority Document(s)
- ☐ Certificate Under 37 CFR § 3.73(b)
- ☐ IDS, PTO-1449, and cited references
- ☒ Return receipt postcard
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawings: __ sheets
- ☐ Maintenance Fee Payment
- ☐ Request for Certificate of Correction
- ☐ Notice of Appeal
- ☐ Express Mail No. ___

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 44 PALO ALTO CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN PATENT DEPARTMENT
FENWICK & WEST LLP
TWO PALO ALTO SQUARE
PALO ALTO CA 94306-9752

EXHIBIT B

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK

APPLICANTS:	Daniel Schreiber and Andrew Goldman
SERIAL NO:	09/397,331
FILED:	September 14, 1999
TITLE:	METHOD AND SYSTEM FOR COPYRIGHT PROTECTION OF DIGITAL IMAGES TRANSMITTED OVER NETWORKS
EXAMINER:	Bryce P. Bonzo
ART UNIT:	2785
ATTY. DKT. NO.:	4692

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to the attention of Examiner Bryce P. Bonzo, Group Art Unit 2785, Commissioner for Patents, Washington, D.C. 20231, on the date shown below:

Dated: 9/13/2000 By: [signature]

Daniel R. Brownstone, Reg. No. P-46,581

COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION:
EXAMINER BRYCE P. BONZO
GROUP ART UNIT 2785

TRANSMITTAL OF CERTIFIED COPIES

SIR:

Attached are the certified copies of the foreign applications from which priority is claimed for this case:

Country:	Israel
Application Number:	127093
Filing Date:	November 16, 1998

Country:	Israel
Application Number:	127869
Filing Date:	December 30, 1998

If the Examiner should have any questions, the Examiner is requested to call the undersigned attorney.

Respectfully submitted,
DANIEL SCHREIBER AND ANDREW GOLDMAN

Dated: Sept 13, 2000

By: _____

Daniel R. Brownstone, Reg. No. P-46,581
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (415) 875-2358
Fax.: (415) 281-1350

EXHIBIT B

חוק הפטנטים, התשכ"ז -- 1967
PATENTS LAW, 5727-1967

בקשה לפטנט
Application for Patent

C:33096

לשימוש הלשכה
For Office Use

מספר: 127869
Number

תאריך: 30 -12- 1998
Date

הוקדם/נדחה
Ante/Post-dates

אני, (שם המבקש, מענו -- ולגבי גוף מאוגד -- מקום התאגדותו)
I (Name and address of applicant, and, in case of body corporate-place of incorporation)

סיסייף בע"מ
ת. ד. 2361
גבעת שרת
בית שמש

CSAFE LTD.
P.O.B. 2361
Givat Sharett
Beit Shemesh

(חברה ישראלית)
(An Israeli company)

בעל אמצאה מכח החוק
of an invention, the title of which is:

ששמה הוא By Law
Owner, by virtue of

(בעברית) הגנה בפני העתקת קבצים ברשת
(Hebrew)

(באנגלית)
NETWORK FILE COPY PROTECTION
(English)

מבקש בזאת כי ינתן לי עליה פטנט
hereby apply for a patent to be granted to me in respect thereof

*בקשה חלוקה - Application for Division	*בקשת פטנט מוסף - Application for Patent of Addition	*דרישה דין קדימה Priority Claim		
מבקשת פטנט from Application	*לבקשה/לפטנט to Patent/Appl.	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
מס. No. _____ מיום dated _____	מס. No. _____ מיום dated _____			
*יפוי כח: כללי/מיוחד - רצוף בזה / עד יוגש P.O.A.: general / individual - attached / to be filed later - הוגש בענין filed in case _____				
המען למסירת הודעות ומסמכים בישראל Address for Service in Israel: Sanford T. Colb & Co., P.O.B. 2273, Rehovot 76122				
חתימת המבקש Signature of Applicant: For the Applicant, Sanford T. Colb & Co. C:33096		This היום 30 of בחודש December 1998 of the year שנת		

לשימוש הלשכה
For Office Use

רשם מאושר
סגן רשם הפטנטים
ירושלים 26.07.2000

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם בספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application, the particulars of which are set out above.

* מחק את המיותר
Delete whatever is inapplicable

EXHIBIT B

הגנה בפני העתקת קבצים ברשת

NETWORK FILE COPY PROTECTION

CSAFE LTD.
C: 33096

סיסייף בע"מ

FIELD OF THE INVENTION

The present invention relates to network security in general and particularly to methods and apparatus for preventing unauthorized copying of files transmitted via computer networks.

BACKGROUND OF THE INVENTION

Preventing unauthorized copying of files transmitted via computer networks is difficult given the current state of the art. Typically, a computer terminal or "client" connected to a network, such as the Internet, sends a request to a "server" also connected to the network. Such requests are often for files known as "web pages," documents constructed using Hypertext Markup Language or HTML, and their associated files which may contain images, sound, or other data. The files are then sent by the server to the client where the files may be output, often using software known as a "browser" which displays web pages, images, and plays sound files. Requested files are typically received at the client in a standard format such as GIF, JPEG, or MIDI and automatically stored at the client, and may be easily copied, pasted, and altered, allowing for unrestricted future reuse, often in violation of copyright laws.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved methods and apparatus for preventing unauthorized copying of files transmitted via computer networks that overcome the known disadvantages of the prior art as discussed above..

There is thus provided in accordance with a preferred embodiment of the present invention a method for preventing unauthorized copying of files sent from a first computer to a second computer. The method comprises the following steps:

(a) sending a request for a file from the second computer to the first computer;

(b) determining at the first computer, in response to the request, whether the file is to be protected and, if so, protecting the file;

(c) sending the protected file to the second computer;

(d) disabling file copying capabilities at the second computer;

(e) unprotecting the file at the second computer; and

(f) outputting the file at the second computer.

In a preferred embodiment any of the sending steps comprises sending via a network.

Preferably the first computer is a server and the second computer is a client.

Preferably the determining step (b) comprises protecting the file by encrypting the file using an encryption key and the unprotecting step (e) comprises decrypting the encrypted file using the encryption key.

In many cases the second computer may be configured with a MICROSOFT WINDOWS operating system. Thus the disabling step (d) comprises trapping any of print screen, bitblt, stretchblt, and getpixel function calls and, in response to the trapping, replacing contents of a clipboard associated with the operating system with substitute contents.

Alternatively or additionally in such a case disabling step (d) comprises trapping any of print screen, bitblt, stretchblt, and getpixel function calls and, in response to the trapping, marring contents of a clipboard associated with the operating system.

Preferably the outputting step (f) comprises displaying the file on a computer monitor.

If appropriate, the outputting step (f) may comprise outputting the file as sound.

The method may comprise the further step of

(g) maintaining at the first computer a list of files to be protected, the determining step (b) comprising determining whether the file requested in step (a) is in the list of files.

In a further embodiment the method comprises the following additional steps prior to the sending a request step (a):

(h) sending a request for an HTML file from the second computer to the first computer;

(i) determining at the first computer, in response to the request, whether the HTML file comprises an instruction to retrieve a file to be protected;

(j) modifying the HTML file by replacing the instruction with an instruction to invoke a protection module for use in retrieving the file to be protected; and

(k) sending the modified HTML file to the second computer.

Preferably, the stage of modifying the HTML file step (h) comprises replacing the name of the file to be protected with a substitute file name.

Preferably, modifying the HTML file step (h) comprises deriving the substitute file name from the name of the file to be protected using a predetermined file name derivation

algorithm.

In one embodiment the procedure is modified as follows,

(l) maintaining at the first computer a mapping of names of files to be protected to corresponding substitute file names, and wherein the determining step (b) comprises determining whether the name of the file requested in step (a) is a substitute file name in the mapping and, if so, protecting the file to be protected corresponding to the substitute file name.

An embodiment further comprises configuring the second computer with the protection module.

Preferably the protection module periodically checks a third computer for an updated component of the protection module and, if found, downloads the updated component.

In an embodiment determining step (b) comprises protecting the file by encrypting the file using an encryption key together with a predetermined hash value incorporated therein, and further comprising configuring the second computer with a protection module operative to hash a software component of the protection module, thereby deriving the predetermined hash value, and incorporate the hash value into the encyption key, and wherein the unprotecting step (e) comprises decrypting the encrypted file using the encryption key together with the derived hash value.

A particularly preferred embodiment further comprises configuring the second computer with a blacklist of known software applications, and wherein the outputting step (f) comprises outputting only if none of the blacklisted applications are currently running on the second computer.

According to a second aspect of the present invention there is provided a method for serving a CGI request by proxy, the method comprising:

sending a CGI request from a client to a server;

forwarding the CGI request from the server to a filter;

appending at the filter an identifier to the CGI request;

sending the CGI request with identifier from the filter to the server;

forwarding the CGI request with identifier from the server to a filter;

removing at the filter the identifier from the CGI request;

sending the CGI request from the filter to a CGI program;

processing the CGI request at the CGI program;

receiving at the server results from the CGI program;

sending the results from the server to the filter;

processing the results at the filter; and

sending the processed results to the client.

According to a third aspect of the present invention there is provided a method for serving an aliased HTTP request, the method comprising:

sending a request for a file from a client to a first server;

issuing a substitute HTTP request corresponding to the requested file to a second server;

receiving at the first server results of the substitute HTTP request;

processing the results at the first server; and

sending the processed results to the client.

It is noted that throughout the specification and claims the term "user" as it is used with respect to the use of a computer may refer to a human or surrogate therefor in combination with the computer with which the human or surrogate interacts. Thus, unless otherwise specified, a reference to a user may connote a reference to the user's computer, and a reference to a user's computer may connote a reference to the user.

It is further noted that throughout the specification and claims the term "file" includes any collection of data that may be stored in a computer memory, on magnetic storage media, or any storage means for use with and/or by a computer.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified block diagram of a system for preventing unauthorized copying of files, the system constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 2A and 2B, taken together, are simplified pictorial flow illustrations of a method of operation of the system of Fig. 1 in accordance with a preferred embodiment of the present invention;

Fig. 3 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention;

Fig. 4 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention;

Fig. 5 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present

invention;

Fig. 6 is a simplified pictorial flow illustration of a file protection method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention; and

Fig. 7 is a simplified pictorial flow illustration of a file protection method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified block diagram of a system for preventing unauthorized copying of files, the system constructed and operative in accordance with a preferred embodiment of the present invention. In the system of Fig. 1 a server 10 is provided for communication with a client 12 via a communications network 14, such as the Internet or an Intranet. Server 10 is typically any known computer configured with web server software and communications software and hardware for communication via network 14 through a socket 16 as is well known. Examples of web server software include Internet Information Server™, commercially available from Microsoft Corporation, and Netscape HTTP Server™, commercially available from Netscape Corporation. Client 12 is typically any known computer configured with a web browser and communications software and hardware for communication via network 14 through a socket 18 as is well known. Examples of web browser software include Internet Explorer™ version 3.02, commercially available from Microsoft Corporation, and Netscape Navigator™ version 2, commercially available from Netscape Corporation.

Server 10 typically includes a storage 20 for storing files, such as HTML, GIF, JPEG, and other files, that server 10 may provide to requesting clients. Server 10 also typically includes a server configuration 22 which indicates to server 10 which client requests are to be forwarded to a filter 24 for processing. Filter 24 preferably refers to a protection map 26 in which a list of files on

storage 20 to be protected may be maintained. Filter 24 also typically maintains an alias map 28 for mapping file aliases to real file names, as well as a cache 30 for storing processed files. Files processed by filter 24 may be sent to client 12 for additional processing by a protection module 32.

A typical operational scenario of the system of Fig. 1 is now described with additional reference to simplified pictorial flow illustrations Figs. 2A and 2B, which are to be taken together. Operation begins with client 12 sending a request to server 10 for an HTML file. The request may be made using known means, such as by selecting a hyperlink to a World Wide Web page using a browser. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the requested file is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 preferably checks protection map 26 to determine whether the requested file is protected or otherwise includes protected elements. For example, in the case of an HTML file, protection map 26 might indicate that the entire file is protected, and thus all files to which the file refers are to be protected. Similarly, protection map 26 might indicate that an entire disk or directory is protected. Alternatively, protection map 26 might indicate the names of specific files which are to be protected, or might simply indicate that the HTML file contains tags such as "<!protect>" and "<!/protect>" bounding a list of tags referring to files to be protected, such as "IMG" tags. If no level of protection is indicated, filter 24 may instruct server 10 to fulfil the request.

Once filter 24 determines that some level of protection is required, filter 24 parses the HTML file and preferably replaces all tags that refer to a protected file with an appropriate substitute tag and related parameters needed to invoke the operation of protection module 32. Such tags may take the form of an "OBJECT" tag where protection module 32 is an ActiveX™ object for use with Internet Explorer™, or an "EMBED" tag where protection module 32 is a plug-in object for use with Internet Explorer™. Filter 24 also preferably substitutes a reference to the real file name of a protected file with a fictitious name that is preferably derivable from the real file name according to a predetermined algorithm in accordance with techniques well known in the art. Filter

24 preferably identifies the type of browser used from the client's request or otherwise in accordance with techniques well known in the art. Where an unsupported browser is detected, filter 24 may perform a contingency action such as replacing the tag with a link to an error message, replacing the file link with a link to an error message, or sending back the original tag with the real file name replaced with a fictitious file name in the same manner as described hereinbelow for protected files. Once the HTML file has been parsed and modified, filter 24 serves the modified file to client 12, typically by writing to socket 16 via which server 10 is currently communicating with client 12.

Upon receiving the modified HTML file, client 12 invokes protection module 32 in accordance with the substituted "OBJECT" or "EMBED" tag. Protection module 32 then requests the protected file from server 10 using the fictitious file name. Once again server 10 checks server configuration 22 and determines that the request is to be forwarded to filter 24. Upon receiving the request filter 24 preferably derives the real file name from the fictitious file name using a predetermined algorithm as described above. Filter 24 then retrieves the file from storage 20 and preferably protects the file by encrypting, encoding, or otherwise modifying the file using a predetermined file protection algorithm, being any suitable algorithm known in the art for this purpose, preferably using an encryption key. Filter 24 may store the protected file in cache 30 for a period of time, allowing the file protection stage to be subsequently skipped and the protected file to be provided from cache 30 should the file be requested later.

Filter 24 then serves the protected file to client 12 where protection module 32 derives the original file using the same or a complementary file unprotection algorithm, and, where used, the same or a complementary encryption key being preconfigured with protection module 32, either hard-coded or derivable by protection module 32 using a key derivation algorithm, or otherwise sent to protection module 32 by filter 24. Protection module 32 then unprotects and displays, plays, presents, or otherwise outputs the original file using known techniques.

Protection module 32 preferably defeats file copying features at the operating system or application software level by disabling the Microsoft Windows™ "Print Screen," "Bitblt," "StretchBlt," or "GetPixel" functions. API calls such as "Bitblt," "StretchBlt," or "GetPixel" are preferably trapped and either prevented from copying and pasting the protected file or allowed to copy and paste a defaced, substituted, or otherwise modified file. "Print Screen" may similarly be disabled by trapping its API calls or by trapping the pressing of the "Print Screen" key and likewise defacing, substituting, or otherwise modifying the contents of the clipboard. Protection module 32 may additionally or alternatively disable file saving features provided by browsers using known techniques.

Reference is now made to Fig. 3 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 3 protection module 32 periodically checks server 10 for updated components corresponding to components of protection module 32, such as DLL files. Upon detecting the existence of an updated component, protection module 32 downloads the updated component for future use with files prepared in accordance with the method of Figs. 2A and 2B. In this manner an updated file preparation algorithm and/or key may be distributed to client 12 subsequent to a similar update of filter 24.

Reference is now made to Fig. 4 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 4 protection module 32 includes a hashing algorithm which may be used to hash software components of protection module 32 in order to derive a hash value. This hash value is preferably known in advance to filter 24 and may be appended or otherwise incorporated into the encyption key, either as is or after applying a modification algorithm to it, and used to prepare the file sent to client 12. Protection module 32 may similarly incorporate the hash value into the encryption key for deriving the original file. As in Fig. 3, protection module 32 may periodically check server 10 for and download an updated

hashing algorithm.

Reference is now made to Fig. 5 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 5 protection module 32 includes a "blacklist" of known software applications known to have features which defeat anti-copying measures taken by protection module 32. Upon detecting that such a blacklisted application is currently running, either by the application's name or by detecting a known footprint for the application, protection module 32 may withhold requesting a protected file, may prevent a protected file from being displayed, played, presented, or otherwise output, and/or may mar the presentation of the file, and may provide a message to the user requiring that the blacklisted application be terminated before the protected file may be presented properly.

Reference is now made to Fig. 6 which is a simplified pictorial flow illustration of a file protection method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 6 client 12 sends a CGI request to server 10. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the request is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 preferably appends a randomly-generated identifier to the CGI request and sends it back to server 10. Server 10 again checks server configuration 22, determines that the request is of the type that is to be processed by filter 24, and passes the CGI request back to filter 24. Filter 24 strips out the randomly-generated identifier and sends the CGI request to a CGI program 34 (Fig. 1) for processing. The CGI program then sends the results to server 10 which forwards the results to filter 24. Filter 24 preferably processes any files or HTML files received from the CGI program as described hereinabove with reference to Figs. 2A and 2B, protecting files as required, and serves the processed files to client 12.

Reference is now made to Fig. 7 which is a simplified pictorial flow illustration of a file protection method for use with the system of Fig. 1 in accordance with another preferred

embodiment of the present invention. In the method of Fig. 7 client 12 sends a request for a file, such as an HTML file, to server 10. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the request is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 then checks alias map 28 to determine if the requested file is actually an alias to be substituted with an HTTP request to server 10 or another server, the identity of which server is maintained in alias map 28 along with the alias file name. If alias map 28 indicates that the file is an alias, filter 24 then issues the subtitiute HTTP request to the server and address indicated in alias map 28. Upon receiving the requested HTML or file, filter 24 then preferably processes the file as described hereinabove with reference to Figs. 2A and 2B, protecting files as required, and serves the processed files to client 12.

It is appreciated that components of the present invention may be implemented in computer hardware, software, or any suitable combination thereof using conventional techniques.

It is appreciated that the steps of the methods described hereinabove need not necessarily be performed in the order shown, and that in fact different implementations of the steps may be employed to yield similar overall results.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the features described hereinabove as well as modifications and variations thereof which would occur to a person of skill in the art upon reading the foregoing description and which are not in the prior art.

EXHIBIT B

CLAIMS

We claim:

1. A method for preventing unauthorized copying of files sent from a first computer to a second computer, the method comprising:

(a) sending a request for a file from said second computer to said first computer;

(b) determining at said first computer, in response to said request, whether said file is to be protected and, if so, protecting said file;

(c) sending said protected file to said second computer;

(d) disabling file copying capabilities at said second computer;

(e) unprotecting said file at said second computer; and

(f) outputting said file at said second computer.

2. A method according to claim 1 wherein any of said sending steps comprises sending via a network.

3. A method according to claim 1 wherein said first computer is a server and said second computer is a client.

4. A method according to claim 1 wherein said determining step (b) comprises protecting said file by encrypting said file using an encryption key and wherein said unprotecting step (e) comprises decrypting said encrypted file using said encryption key.

5. A method aecording to claim 1 wherein said second computer is configured with a MICROSOFT WINDOWS operating system and wherein said disabling step (d) comprises trapping any of print screen, bitblt, stretchblt, and getpixel function calls and, in response to said trapping,

replacing contents of a clipboard associated with said operating system with substitute contents.

6. A method according to claim 1 wherein said second computer is configured with a MICROSOFT WINDOWS operating system and wherein said disabling step (d) comprises trapping any of print screen, bitblt, stretchblt, and getpixel function calls and, in response to said trapping, marring contents of a clipboard associated with said operating system.

7. A method according to claim 1 wherein said outputting step (f) comprises displaying said file on a computer monitor.

8. A method according to claim 1 wherein said outputting step (f) comprises outputting said file as sound.

9. A method according to claim 1 and further comprising:

(g) maintaining at said first computer a list of files to be protected, and wherein said determining step (b) comprises determining whether said file requested in step (a) is in said list of files.

10. A method according to claim 1 and further comprising:

prior to said sending a request step (a):

(h) sending a request for an HTML file from said second computer to said first computer;

(i) determining at said first computer, in response to said request, whether said HTML file comprises an instruction to retrieve a file to be protected;

(j) modifying said HTML file by replacing said instruction with an instruction to invoke a protection module for use in retrieving said file to be protected; and

modified HTML file to said second computer.

ethod according to claim 10 wherein said modifying said HTML file step (h)
acing the name of said file to be protected with a substitute file name.

12. A method according to claim 11 wherein said modifying said HTML file step (h) comprises deriving said substitute file name from said name of said file to be protected using a predetermined file name derivation algorithm.

3. A method according to claim 11 and further comprising:

(l) maintaining at said first computer a mapping of names of files to be tected to corresponding substitute file names, and wherein said determining step (b) comprises mining whether the name of said file requested in step (a) is a substitute file name in said ng and, if so, protecting said file to be protected corresponding to said substitute file name.

A method according to claim 10 and further comprising configuring said second with said protection module.

A method according to claim 14 wherein said protection module periodically checks er for an updated component of said protection module and, if found, downloads said ient.

nethod according to claim 1 wherein said determining step (b) comprises by encrypting said file using an encryption key together with a predetermined ed therein, and further comprising configuring said second computer with a rative to hash a software component of said protection module, thereby

(k) sending said modified HTML file to said second computer.

11. A method according to claim 10 wherein said modifying said HTML file step (h) comprises replacing the name of said file to be protected with a substitute file name.

12. A method according to claim 11 wherein said modifying said HTML file step (h) comprises deriving said substitute file name from said name of said file to be protected using a predetermined file name derivation algorithm.

13. A method according to claim 11 and further comprising:

(l) maintaining at said first computer a mapping of names of files to be protected to corresponding substitute file names, and wherein said determining step (b) comprises determining whether the name of said file requested in step (a) is a substitute file name in said mapping and, if so, protecting said file to be protected corresponding to said substitute file name.

14. A method according to claim 10 and further comprising configuring said second computer with said protection module.

15. A method according to claim 14 wherein said protection module periodically checks a third computer for an updated component of said protection module and, if found, downloads said updated component.

16. A method according to claim 1 wherein said determining step (b) comprises protecting said file by encrypting said file using an encryption key together with a predetermined hash value incorporated therein, and further comprising configuring said second computer with a protection module operative to hash a software component of said protection module, thereby

deriving said predetermined hash value, and incorporate said hash value into said encyption key, and wherein said unprotecting step (e) comprises decrypting said encrypted file using said encryption key together with said derived hash value.

17. A method according to claim 1 and further comprising:

configuring said second computer with a blacklist of known software applications, and wherein said outputting step (f) comprises outputting only if none of said blacklisted applications are currently running on said second computer.

18. A method for serving a CGI request by proxy, the method comprising:

sending a CGI request from a client to a server;

forwarding said CGI request from said server to a filter;

appending at said filter an identifier to the CGI request;

sending said CGI request with identifier from said filter to said server;

forwarding said CGI request with identifier from said server to a filter;

removing at said filter said identifier from said CGI request;

sending said CGI request from said filter to a CGI program;

processing said CGI request at said CGI program;

receiving at said server results from said CGI program;

sending said results from said server to said filter;

processing said results at said filter; and

sending said processed results to said client.

19. A method for serving an aliased HTTP request, the method comprising:

sending a request for a file from a client to a first server;

issuing a substitute HTTP request corresponding to said requested file to a second server;

receiving at said first server results of said substitute HTTP request;

processing said results at said first server; and

sending said processed results to said client.

20. A method substantially as shown and described above.

21. A method substantially as illustrated in any of the drawings.

For the Applicant,

Sanford T. Colb & Co.
C:33096

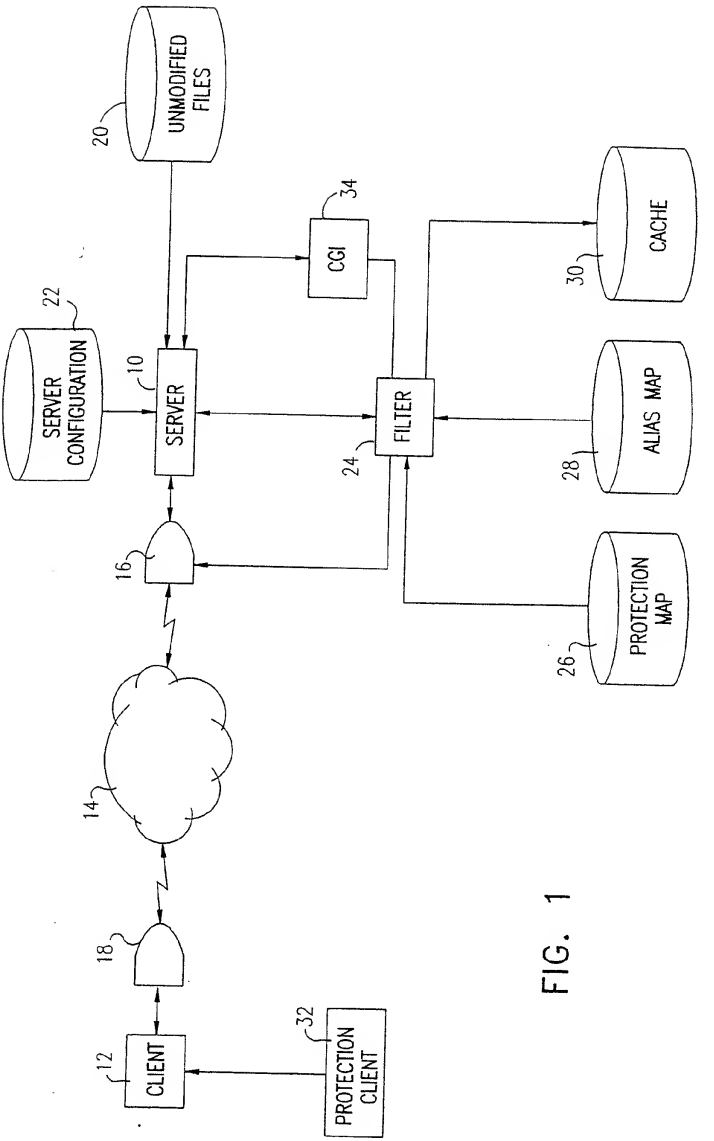

UNMODIFIED FILES
20
CGI
34
CACHE
30
SERVER CONFIGURATION
22
SERVER
10
FILTER
24
ALIAS MAP
28
16
PROTECTION MAP
26
14
18
CLIENT
12
PROTECTION CLIENT
32

FIG. 1

FIG. 2A

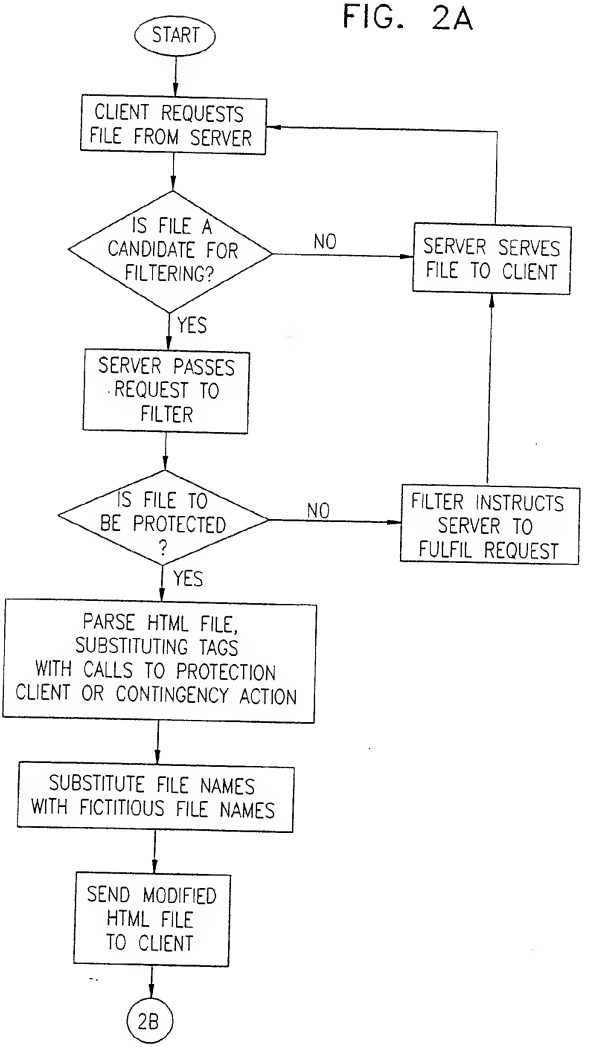

START
CLIENT REQUESTS FILE FROM SERVER
IS FILE A CANDIDATE FOR FILTERING?
NO
SERVER SERVES FILE TO CLIENT
YES
SERVER PASSES REQUEST TO FILTER
IS FILE TO BE PROTECTED ?
NO
FILTER INSTRUCTS SERVER TO FULFIL REQUEST
YES
PARSE HTML FILE, SUBSTITUTING TAGS WITH CALLS TO PROTECTION CLIENT OR CONTINGENCY ACTION
SUBSTITUTE FILE NAMES WITH FICTITIOUS FILE NAMES
SEND MODIFIED HTML FILE TO CLIENT
2B

FIG. 2B

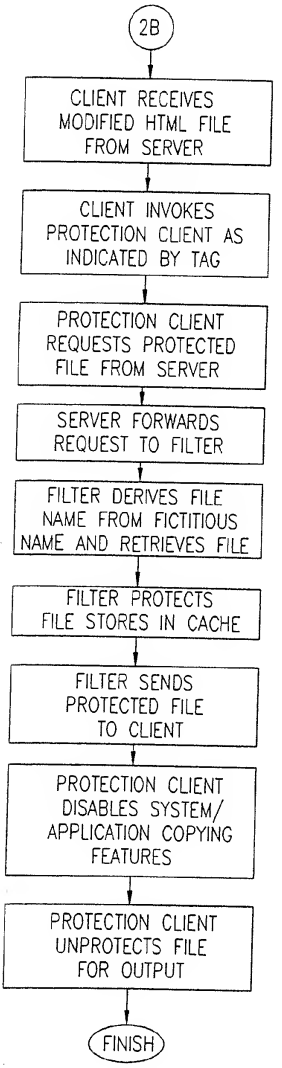

2B
CLIENT RECEIVES MODIFIED HTML FILE FROM SERVER
CLIENT INVOKES PROTECTION CLIENT AS INDICATED BY TAG
PROTECTION CLIENT REQUESTS PROTECTED FILE FROM SERVER
SERVER FORWARDS REQUEST TO FILTER
FILTER DERIVES FILE NAME FROM FICTITIOUS NAME AND RETRIEVES FILE
FILTER PROTECTS FILE STORES IN CACHE
FILTER SENDS PROTECTED FILE TO CLIENT
PROTECTION CLIENT DISABLES SYSTEM/ APPLICATION COPYING FEATURES
PROTECTION CLIENT UNPROTECTS FILE FOR OUTPUT
FINISH

FIG. 3

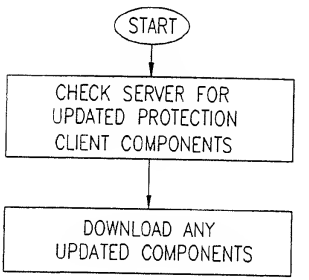

START
CHECK SERVER FOR UPDATED PROTECTION CLIENT COMPONENTS
DOWNLOAD ANY UPDATED COMPONENTS

FIG. 4

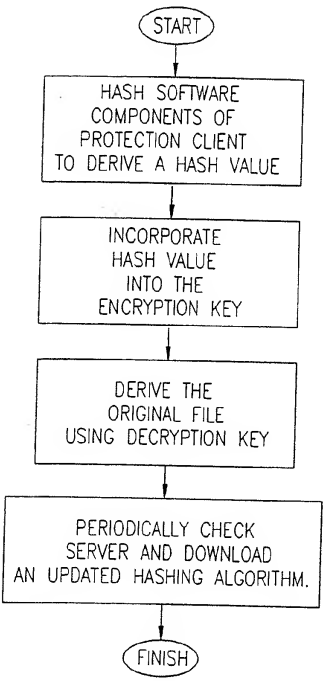
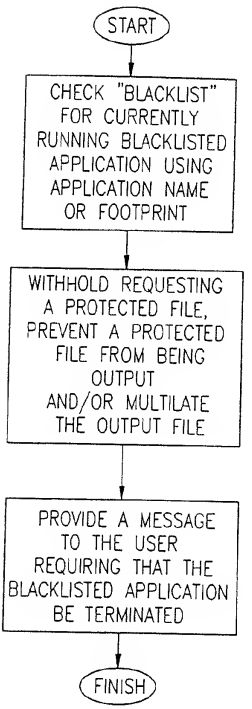

START
HASH SOFTWARE COMPONENTS OF PROTECTION CLIENT TO DERIVE A HASH VALUE
INCORPORATE HASH VALUE INTO THE ENCRYPTION KEY
DERIVE THE ORIGINAL FILE USING DECRYPTION KEY
PERIODICALLY CHECK SERVER AND DOWNLOAD AN UPDATED HASHING ALGORITHM.
FINISH

FIG. 5


START
CHECK "BLACKLIST" FOR CURRENTLY RUNNING BLACKLISTED APPLICATION USING APPLICATION NAME OR FOOTPRINT
WITHHOLD REQUESTING A PROTECTED FILE, PREVENT A PROTECTED FILE FROM BEING OUTPUT AND/OR MULTILATE THE OUTPUT FILE
PROVIDE A MESSAGE TO THE USER REQUIRING THAT THE BLACKLISTED APPLICATION BE TERMINATED
FINISH

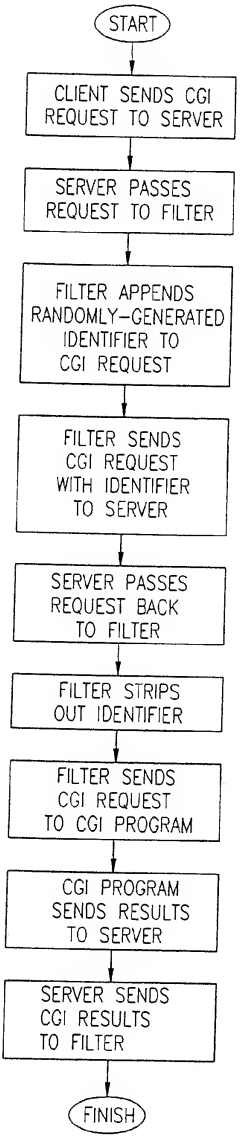

START
CLIENT SENDS CGI REQUEST TO SERVER
SERVER PASSES REQUEST TO FILTER
FILTER APPENDS RANDOMLY-GENERATED IDENTIFIER TO CGI REQUEST
FILTER SENDS CGI REQUEST WITH IDENTIFIER TO SERVER
SERVER PASSES REQUEST BACK TO FILTER
FILTER STRIPS OUT IDENTIFIER
FILTER SENDS CGI REQUEST TO CGI PROGRAM
CGI PROGRAM SENDS RESULTS TO SERVER
SERVER SENDS CGI RESULTS TO FILTER
FINISH

FIG. 6

FIG. 7

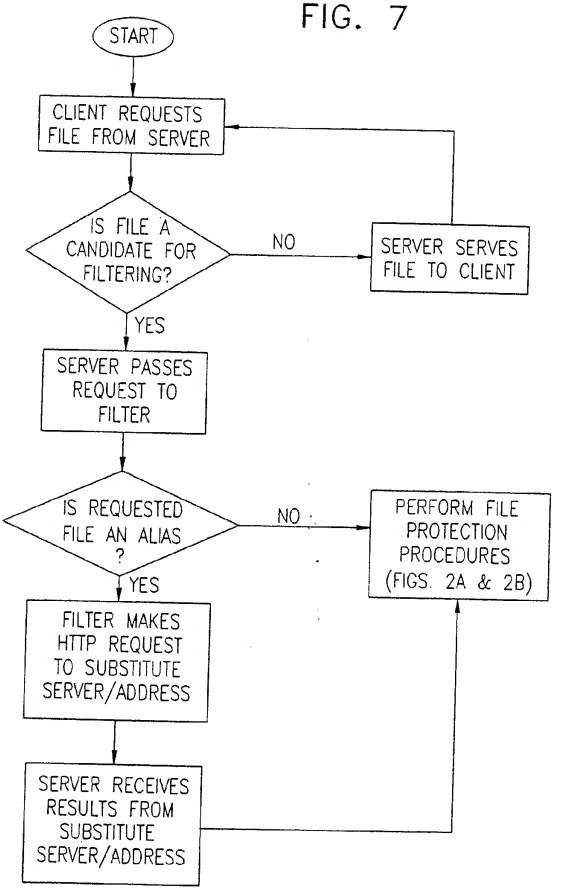

START
CLIENT REQUESTS FILE FROM SERVER
IS FILE A CANDIDATE FOR FILTERING?
NO
SERVER SERVES FILE TO CLIENT
YES
SERVER PASSES REQUEST TO FILTER
IS REQUESTED FILE AN ALIAS ?
NO
PERFORM FILE PROTECTION PROCEDURES (FIGS. 2A & 2B)
YES
FILTER MAKES HTTP REQUEST TO SUBSTITUTE SERVER/ADDRESS
SERVER RECEIVES RESULTS FROM SUBSTITUTE SERVER/ADDRESS

EXHIBIT B

לשימוש הלשכה
For Office Use

מספר: Number	127093
תאריך: Date	16-11-1998
הוקדם/נדחה Ante/Post-dates	

תוק הפטנטים, התשכ"ז -- 1967
PATENTS LAW, 5727-1967

בקשה לפטנט
Application for Patent

C:32789

אני, (שם המבקש, מענו -- ולגבי גוף מאוגד -- מקום התאגדותו)
I (Name and address of applicant, and, in case of body corporate-place of incorporation)

CSAFE LTD.
P.O.B. 2361
Givat Sharett
Beit Shemesh

(An Israeli Company)

סיסייף בע"מ
ת.ד. 2361
גבעת שרת
בית שמש

(חברה ישראלית)

Owner, by virtue of שמשמה הוא By Law

בעל אמצאה מכח הדין
of an invention, the title of which is:

(Hebrew) הגנה מפני העתקה

(English) COPY PROTECTION

hereby apply for a patent to be granted to me in respect thereof מבקש בזאת כי יינתן לי עליה פטנט

*בקשה חלוקה - Application for Division	*בקשת פטנט מוסף - Application for Patent of Addition	*דרישה דין קדימה Priority Claim		
מבקשת פטנט from Application	*לבקשה/לפטנט to Patent/Appl.	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
No. מס.	No. מס.			
dated מיום	dated מיום			
*יפוי כח: כללי/מיוחד - רצוף בזה / עוד יוגש P.O.A.: general / individual - attached / to be filed later - filed in case הוגש בעניין				

	המען למסירת הודעות ומסמכים בישראל Address for Service in Israel Sanford T. Colb & Co. P.O.B. 2273 Rehovot 76122
חתימת המבקש Signature of Applicant For the Applicant, Sanford T. Colb & Co. C:32789	היום This 16 בחודש of November שנת of the year 1998

לשימוש הלשכה
For Office Use

רשם הפטנטים
26.11.98

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם בספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application, the particulars of which are set out above.

EXHIBIT B

הגנה מפני העתקה

COPY PROTECTION

CSAFE LTD.
C: 32789

סיסייף בע"מ

FIELD OF THE INVENTION

The present invention relates to network security in general and particularly to methods and apparatus for preventing unauthorized copying of images transmitted via computer networks.

BACKGROUND OF THE INVENTION

Preventing unauthorized copying of images transmitted via computer networks is difficult given the current state of the art. Typically, a computer terminal or "client" connected to a network, such as the Internet, sends a request using software known as a "browser" to a "server" also connected to the network. Such requests are often for "Web pages," documents constructed using Hypertext Markup Language or HTML, and their associated images which are then sent by the server and rendered by the client browser for viewing. Images are typically received at the client in a standard format such as GIF or JPEG, are automatically stored at the client, and may be easily copied and pasted, allowing for unrestricted future reuse, often in violation of copyright laws.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved methods and apparatus for preventing unauthorized copying of images transmitted via computer networks that overcome the known disadvantages of the prior art as discussed above..

There is thus provided in accordance with a preferred embodiment of the present invention a method for preventing unauthorized copying of images, the method including protecting an image file on a first computer using a protection algorithm, providing the protected image to a

second computer, disabling image copying functions on the second computer, and unprotecting the protected image on the second computer for display using an unprotection algorithm.

Further in accordance with a preferred embodiment of the present invention the protecting step includes protecting using an encryption key.

Still further in accordance with a preferred embodiment of the present invention the encryption key includes a hash value component.

Additionally in accordance with a preferred embodiment of the present invention the method further includes modifying an HTML file that includes at least one link to the protected image by substituting IMG tags of protected images with calls to image unprotection software on the second computer.

Further in accordance with a preferred embodiment of the present invention the modifying step includes replacing file names of the protected images with derived file names using a file name derivation algorithm.

It is noted that throughout the specification and claims the term "user" as it is used with respect to the use of a computer may refer to a human or surrogate therefor in combination with the computer interface with which the human or surrogate interacts. Thus, unless otherwise specified, a reference to a user may connote a reference to the user's computer interface, and a reference to a user's computer interface may connote a reference to the user.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified block diagram of a system for preventing unauthorized copying of images, the system constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 2A and 2B, taken together, are simplified pictorial flow illustrations of a method of operation of the system of Fig. 1 in accordance with a preferred embodiment of the present invention;

Fig. 3 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention;

Fig. 4 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention;

Fig. 5 is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention;

Fig. 6 is a simplified pictorial flow illustration of an image protection method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention; and

Fig. 7 is a simplified pictorial flow illustration of an image protection method for use with the system of Fig. 1 operative in accordance with another preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified block diagram of a system for preventing unauthorized copying of images, the system constructed and operative in accordance with a preferred embodiment of the present invention. In the system of Fig. 1 a server 10 is provided for communication with a client 12 via a communications network 14, such as the Internet or an Intranet. Server 10 is typically any known computer configured with web server software and communications software and hardware for communication via network 14 through a socket 16 as

is well known. Examples of web server software include Internet Information Server™, commercially available from Microsoft Corporation, and Netscape HTTP Server™, commercially available from Netscape Corporation. Client 12 is typically any known computer configured with a web browser and communications software and hardware for communication via network 14 through a socket 18 as is well known. Examples of web browser software include Internet Explorer™ version 3.02, commercially available from Microsoft Corporation, and Netscape Navigator™ version 2, commercially available from Netscape Corporation.

Server 10 typically includes a storage 20 for storing files, such as HTML, GIF, JPEG, and other files, that server 10 may provide to requesting clients. Server 10 also typically includes a server configuration 22 which indicates to server 10 which client requests are to be forwarded to a filter 24 for processing. Filter 24 preferably refers to a protection map 26 in which a list of files on storage 20 to be protected may be maintained. Filter 24 also typically maintains an alias map 28 for mapping file aliases to real file names, as well as a cache 30 for storing processed image files. Files processed by filter 24 may be sent to client 12 for additional processing by an image client 32.

A typical operational scenario of the system of Fig. 1 is now described with additional reference to simplified pictorial flow illustrations Figs. 2A and 2B, which are to be taken together. Operation begins with client 12 sending a request to server 10 for an HTML file. The request may be made using known means, such as by selecting a hyperlink to a World Wide Web page using a browser. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the requested file is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 preferably checks protection map 26 to determine whether the requested file is protected or otherwise includes protected elements. For example, in the case of an HTML file, protection map 26 might indicate that the entire file is protected, and thus all images to which the file refers are to be protected. Similarly, protection map 26 might indicate that an entire disk or directory is protected. Alternatively, protection map 26 might indicate the names of specific image files which are to be protected, or might simply indicate

that the HTML file contains tags such as "<!protect>" and "<!/protect>" bounding a list of "IMG" tags with images to be protected. If no level of protection is indicated, filter 24 may instruct server 10 to fulfil the request.

Once filter 24 determines that some level of protection is required, filter 24 parses the HTML file and preferably replaces all "IMG" tags associated with a protected image with an appropriate substitute tag and related parameters needed to invoke the operation of image client 32. Such tags may take the form of an "OBJECT" tag where image client 32 is an ActiveX™ object for use with Internet Explorer™, or an "EMBED" tag where image client 32 is a plug-in object for use with Internet Explorer™. Filter 24 also preferably substitutes a reference to the real file name of a protected image with a fictitious name that is preferably derivable from the real file name according to a predetermined algorithm in accordance with techniques well known in the art. Filter 24 preferably identifies the type of browser used from the client's request or otherwise in accordance with techniques well known in the art. Where an unsupported browser is detected, filter 24 may perform a contingency action such as replacing the "IMG" tag with a link to an error message, replacing the image link with a link to an error message image, or sending back the original "IMG" tag with the real image file name replaced with a fictitious image file name in the same manner as described hereinbelow for protected images. Once the HTML file has been parsed and modified, filter 24 serves the modified file to client 12, typically by writing to socket 16 via which server 10 is currently communicating with client 12.

Upon receiving the modified HTML file, client 12 invokes image client 32 in accordance with the substituted "OBJECT" or "EMBED" tag. Image client 32 then requests the protected image from server 10 using the fictitious image file name. Once again server 10 checks server configuration 22 and determines that the request is to be forwarded to filter 24. Upon receiving the request filter 24 preferably derives the real image file name from the fictitious image file name using a predetermined algorithm as described above. Filter 24 then retrieves the image file from storage 20 and preferably protects the image by encrypting, encoding, or otherwise

modifying the image file using a predetermined image protection algorithm, being any suitable algorithm known in the art for this purpose, preferably using an encryption key. Filter 24 may store the protected image in cache 30 for a period of time, allowing the image file protectionstage to be subsequently skipped and the protected image file to be provided from cache 30 should the image be requested later.

Filter 24 then serves the protected image to client 12 where image client 32 derives the original image using the same or a complementary image unprotection algorithm, and, where used, the same or a complementary encryption key being preconfigured with image client 32, either hard-coded or derivable by image client 32 using a key derivation algorithm, or otherwise sent to image client 32 by filter 24. Image client 32 then unprotects and displays the original image using known techniques.

Image client 32 preferably defeats image copying features at the operating system or application software level by disabling the Microsoft Windows™ "Print Screen," "Bitblt," "StretchBlt," or "GetPixel" functions. API calls such as "Bitblt," "StretchBlt," or "GetPixel" are preferably trapped and either prevented from copying and pasting the protected image or allowed to copy and paste a defaced, substituted, or otherwise modified image. "Print Screen" may similarly be disabled by trapping its API calls or by trapping the pressing of the "Print Screen" key and likewise defacing, substituting, or otherwise modifying the contents of the clipboard. Image client 32 may additionally or alternatively disable image saving features provided by browsers using known techniques.

Reference is now made to Fig. 3 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 3 image client 32 periodically checks server 10 for updated components corresponding to components of image client 32, such as DLL files. Upon detecting the existence of an updated component, image client 32 downloads the updated component for future use with images prepared in accordance with the method of Figs. 2A

and 2B. In this manner an updated image preparation algorithm and/or key may be distributed to client 12 subsequent to a similar update of filter 24.

Reference is now made to Fig. 4 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 4 image client 32 includes a hashing algorithm which may be used to hash software components of image client 32 in order to derive a hash value. This hash value is preferably known in advance to filter 24 and may be appended or otherwise incorporated into the encyption key, either as is or after applying a modification algorithm to it, and used to prepare the image file sent to client 12. Image client 32 may similarly incorporate the hash value into the encryption key for deriving the original image. As in Fig. 3, image client 32 may periodically check server 10 for and download an updated hashing algorithm.

Reference is now made to Fig. 5 which is a simplified pictorial flow illustration of an anti-hacking method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 5 image client 32 includes a "blacklist" of known software applications known to have features which defeat anti-copying measures taken by image client 32. Upon detecting that such a blacklisted application is currently running, either by the application's name or by detecting a known footprint for the application, image client 32 may withhold requesting a protected image, may prevent a protected from being displayed, and/or may mutilate the displayed image, and may provide a message to the user requiring that the blacklisted application be terminated before the protected image may be viewed properly.

Reference is now made to Fig. 6 which is a simplified pictorial flow illustration of an image protection method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 6 client 12 sends a CGI request to server 10. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the request is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 preferably appends a randomly-generated identifier to the CGI

request and sends it back to server 10. Server 10 again checks server configuration 22, determines that the request is of the type that is to be processed by filter 24, and passes the CGI request back to filter 24. Filter 24 strips out the randomly-generated identifier and sends the CGI request to a CGI program 34 (Fig. 1) for processing. The CGI program then sends the results to server 10 which forwards the results to filter 24. Filter 24 preferably processes any image files or HTML files received from the CGI program as described hereinabove with reference to Figs. 2A and 2B, protecting image files as required, and serves the processed files to client 12.

Reference is now made to Fig. 7 which is a simplified pictorial flow illustration of an image protection method for use with the system of Fig. 1 in accordance with another preferred embodiment of the present invention. In the method of Fig. 7 client 12 sends a request for a file, such as an HTML file, to server 10. Upon receiving the request from client 12, server 10 checks server configuration 22 to determine whether the request is of the type that is to be processed by filter 24 and, if it is, passes the request to filter 24. Filter 24 then checks alias map 28 to determine if the requested file is actually an alias to be substituted with an HTTP request to server 10 or another server, the identity of which server is maintained in alias map 28 along with the alias file name. If alias map 28 indicates that the file is an alias, filter 24 then issues the subtitiute HTTP request to the server and address indicated in alias map 28. Upon receiving the requested HTML or image file, filter 24 then preferably processes the file as described hereinabove with reference to Figs. 2A and 2B, protecting image files as required, and serves the processed files to client 12.

It is appreciated that components of the present invention may be implemented in computer hardware, software, or any suitable combination thereof using conventional techniques.

It is appreciated that the steps of the methods described hereinabove need not necessarily be performed in the order shown, and that in fact different implementations of the steps may be employed to yield similar overall results.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the

present invention includes both combinations and subcombinations of the features described hereinabove as well as modifications and variations thereof which would occur to a person of skill in the art upon reading the foregoing description and which are not in the prior art.

We claim:

1. A method for preventing unauthorized copying of images, the method comprising:

protecting an image file on a first computer using a protection algorithm;

providing said protected image to a second computer;

disabling image copying functions on said second computer; and

unprotecting said protected image on said second computer for display using an unprotection algorithm.

2. A method according to claim 1 wherein said protecting step comprises protecting using an encryption key.

3. A method according to claim 2 wherein said encryption key comprises a hash value component.

4. A method according to claim 1 and further comprising modifying an HTML file that comprises at least one link to said protected image by substituting IMG tags of protected images with calls to image unprotection software on said second computer.

5. A method according to claim 4 wherein said modifying step comprises replacing file names of said protected images with derived file names using a file name derivation algorithm.

6. A method substantially as shown and described above.

7. A method substantially as illustrated in any of the drawings.

For the Applicant,

Sanford T. Colb & Co.
C:32789

UNMODIFIED FILES
20
CGI
34
CACHE
30
ALIAS MAP
28
10
SERVER CONFIGURATION
SERVER
FILTER
PROTECTION MAP
22
24
26
16
14
18
CLIENT
12
IMAGE CLIENT
32

FIG. 1

EXHIBIT B

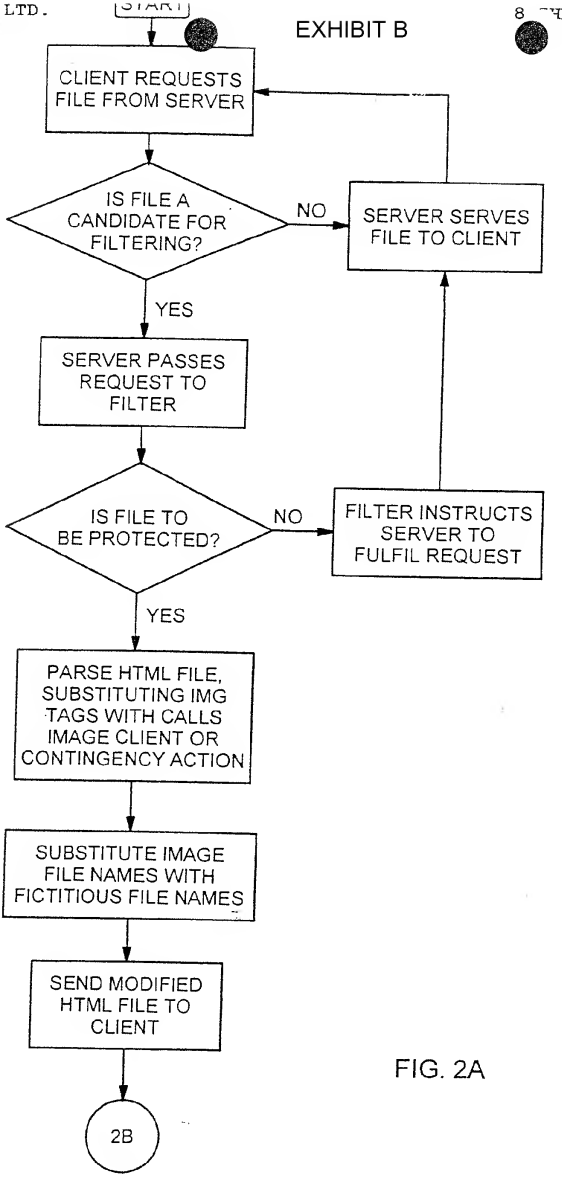


FIG. 2A

EXHIBIT B

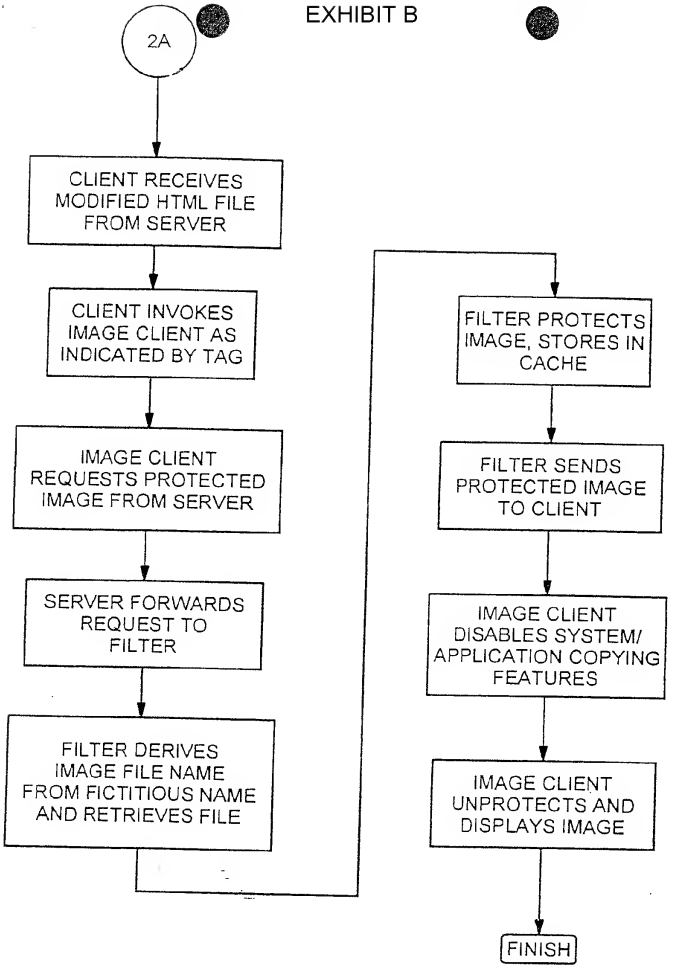


FIG. 2B

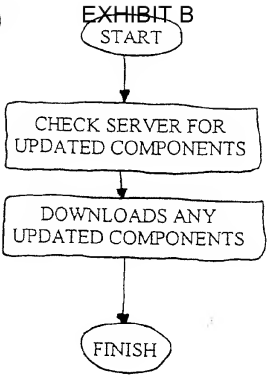


EXHIBIT B
START
CHECK SERVER FOR UPDATED COMPONENTS
DOWNLOADS ANY UPDATED COMPONENTS
FINISH

Fig. 3

EXHIBIT B

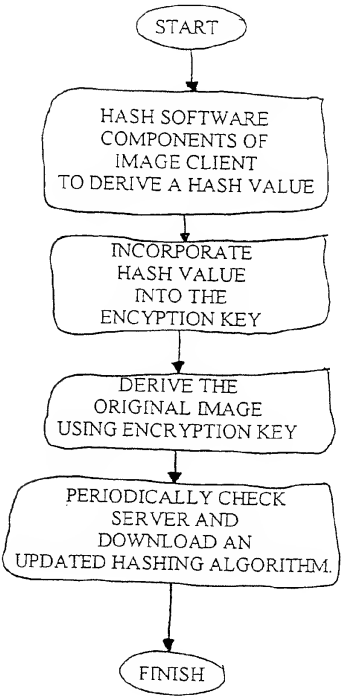


Fig. 4

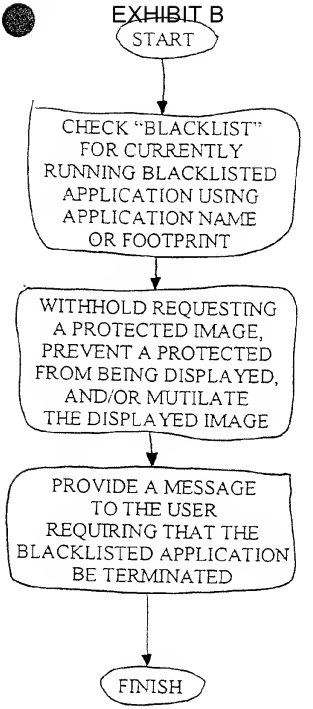


EXHIBIT B
START
CHECK "BLACKLIST" FOR CURRENTLY RUNNING BLACKLISTED APPLICATION USING APPLICATION NAME OR FOOTPRINT
WITHHOLD REQUESTING A PROTECTED IMAGE, PREVENT A PROTECTED FROM BEING DISPLAYED, AND/OR MUTILATE THE DISPLAYED IMAGE
PROVIDE A MESSAGE TO THE USER REQUIRING THAT THE BLACKLISTED APPLICATION BE TERMINATED
FINISH

Fig. 5

EXHIBIT B

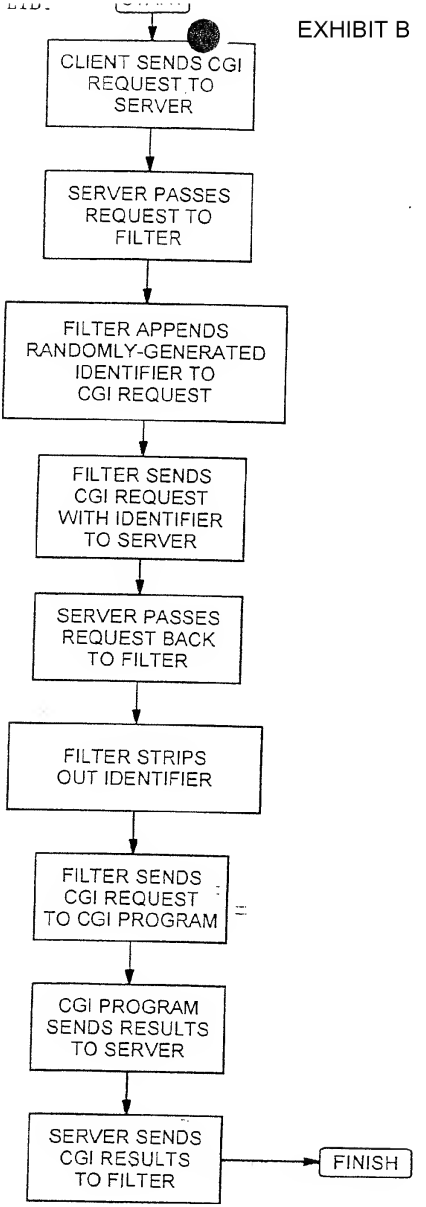


FIG. 6

EXHIBIT B

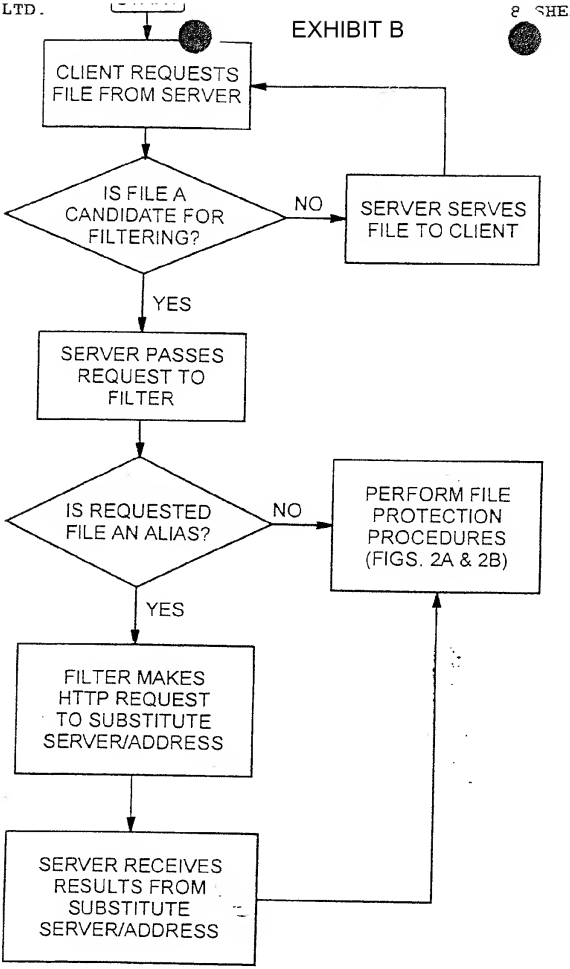


FIG. 7

EXHIBIT C

4692US

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

RECEIVED
MAY 07 2001
FENWICK & WEST LLP

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED

First Named Applicant

TITLE OF INVENTION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or
B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number.
Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibillty to ensure timely payment of maintenance fees when due.

YOUR COPY

EXHIBIT C

Notice of Allowability	Application No. 09/397,331	Applicant(s) SCHREIBER ET AL.
	Examiner Bryce P Bonzo	Art Unit 2184

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment C of 4/23/01*.
2. ☒ The allowed claim(s) is/are *151-162*.
3. ☐ The drawings filed on _____ are acceptable as formal drawings.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
   1. ☒ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____.
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.
5. ☒ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE FOR SUBMITTING NEW FORMAL DRAWINGS , OR A SUBSTITUTE OATH OR DECLARATION. This three-month period for complying with the REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL is extendable under 37 CFR 1.136(a).**

6. ☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

7. ☒ Applicant MUST submit NEW FORMAL DRAWINGS
   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review(PTO-948) attached
   1) ☐ hereto or 2) ☒ to Paper No. *16*.
   (b) ☐ including changes required by the proposed drawing correction filed _____, which has been approved by the examiner.
   (c) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No. _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftsperson.

8. ☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any reply to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE / SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

1☐ Notice of References Cited (PTO-892)
2☐ Notice of Informal Patent Application (PTO-152)
3☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
4☐ Interview Summary (PTO-413), Paper No.____.
5☐ Information Disclosure Statements (PTO-1449), Paper No. ____.
6☐ Examiner's Amendment/Comment
7☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
8☐ Examiner's Statement of Reasons for Allowance
9☐ Other

ROBERT BEAUSOLEIL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXHIBIT C

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

Dear Patent and Trademark Office Customer:

The Technical Support Staff of Technology Center 2100 has undertaken continuous quality improvement efforts to ensure that the accompanying correspondence meets high quality standards, and focuses on good customer service. It is important to us that you are satisfied with the services we provide.

If the contents of the attached correspondence has any clerical omissions, e.g., missing references or pages, illegible text, other problems or concerns of this nature which you wish to bring to my attention, please call or fax me as soon as possible. I will take the appropriate action to expedite the necessary corrections.

Verlene D. Green
Head,Supervisory Legal Instruments Examiner
Technology Center 2100
(703) 305-4376

Fax No. (703) 308-9051 or (703) 308-9052

Attention: Policy on Returning Phone Calls

A PTO-wide customer service standard is if a PTO employee being called is not available, they will return your call by the next business day, or, if you request, an alternate point of contact will be provided. Technology Center 2100 is committed to meeting this service standard. If you have called any employee in our Technology Center and have not received a return phone call within one (1) business day or have not been provided another point of contact, please contact the Technology Center at 703-306-5631. We ensure that you will receive a return phone call from an employee with the ability to assist you, within four (4) business hours of this contact. We appreciate your help in assisting us to help you.

EXHIBIT D

PATENT
DOCKET NO.: 6866-101XX/993057

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Daniel SCHREIBER et al.

U. S. Serial No.: 09/313,067

Filed: May 17, 1999

For: **METHODS AND APPARATUS FOR PREVENTING REUSE OF TEXT, IMAGES AND SOFTWARE TRANSMITTED VIA NETWORKS**

LETTER

COMMISSIONER OF
PATENTS AND TRADEMARKS
Washington, D. C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Israeli Patent Application No. 124,895 from which priority is claimed under 35 U.S.C. 119 and Rule 55b.

Respectfully submitted,

By_____
Robert Berliner, Esq.
Registration No. 20,121

July 6, 1999

FULBRIGHT & JAWORSKI L.L.P.
865 S. Figueroa Street, 29th Floor
Los Angeles, California 90017
Telephone: (213) 892-9200
Facsimile: (213) 680-4518

EXHIBIT D

STATE PF ISRAEL

s to certify that
an bereto is a true
opy e documents as
igin deposited with
e pa application
icula which are
fied t first page

זאת לתעודה כי
רצופים בזה העתקים
נכונים של המסמכים
שחופקדו לכתחילה
עם הבקשה לפטנט
לפי הפרטים הרשומים
בעמוד הראשון של
הנספח.

This 09 -06- 1999 היום

רשם הפטנטים
Registrar of Patents

EXHIBIT D

לשימוש הלשכה
For Office Use

מספר: Number	124695
תאריך: Date	14-06-1998
הוקדם/נדחה Ante/Post-dates	

תוק הפטנטים, התשכ"ז -- 1967
PATENTS LAW, 5727-1967

בקשה לפטנט
Application for Patent

C:31234

אני, (שם המבקש, מענו -- ולגבי גוף מאוגד -- מקום התאגדותו)
I (Name and address of applicant, and, in case of body corporate-place of incorporation)

CSAFE LTD.
P.O. Box 2361
Beit Shemesh 99000

(An Israel company)

סיסייף בע"מ
ת.ד. 2361
בית שמש 99000

(חברה ישראלית)

בעל אמצאה מכח חדין ששמה הוא By Law
Owner, by virtue of

of an invention, the title of which is:

(בעברית) שיטות והתקן למניעת שימוש חוזר של מלל, תמונות, ותוכנות ששודרו דרך רשתות
(Hebrew)

(באנגלית) METHODS AND APPARATUS FOR PREVENTING REUSE OF TEXT, IMAGES AND SOFTWARE TRANSMITTED VIA NETWORKS
(English)

hereby apply for a patent to be granted to me in respect thereof מבקש בזאת כי ינתן לי עליה פטנט

*בקשה חלוקה - Application for Division	*בקשת פטנט מוסף - Application for Patent of Addition	*דרישה דין קדימה Priority Claim		
מבקשת פטנט from Application	*לבקשה/לפטנט to Patent/Appl.	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
No. מס.	No. מס.			
dated מיום	dated מיום			

*יפוי כח: כללי/מיוחד - רצוף בזה / עוד יוגש
P.O.A.: general / individual - attached / to be filed later -

filed in case הוגש בענין

המען למסירת הודעות ומסמכים בישראל
Address for Service in Israel

Sanford T. Colb & Co.
P.O.B. 2273
Rehovot 76122

תתימת המבקש
Signature of Applicant

For the Applicant,

Sanford T. Colb & Co.
C:31234

היום 14 בחודש JUNE שנת 1998
This of the year

לשימוש הלשכה
For Office Use

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם בספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application,